REMARKS

Applicants wish to thank the Examiner for reviewing the present application.

Applicants advise that a change of correspondence address is being filed with this response. Applicants also advise that the attorney docket number for the present application has changed, and the new attorney docket number is noted above. Applicants kindly request that the Office amend its records to indicate same.

Amendments to the Specification

The specification is amended to correct typographical errors found in a formula. No new matter is believed to be added by way of this amendment.

Amendments to the Claims

Claim 1 is amended to correct various typographical errors, and to better reflect the physical transformation of the various elements recited therein for generating a shared key.

Claims 2-8 are added in this response. Claims 2-8 recite additional embodiments dependent on the method recited in claim 1. Support for these claims can be found in paragraphs [0043] to [0049] and paragraphs [0051] to [0057] of the specification as published.

No new matter is believed to be added by way of these amendments.

Claim Rejections – 35 U.S.C. §112, second paragraph

Claim 1 was rejected under 35 U.S.C. §112, second paragraph for insufficient antecedence basis for the expressions "said first short term private key", "said first long term private key, and "said second long term public key". These expressions have been amended replacing "said" with "a" where appropriate. Therefore, claim 1 is submitted to comply with 35 U.S.C. §112, second paragraph.

Claim Rejections – 35 U.S.C. §101

Claim 1 was rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Claim 1 is amended to better reflect the physical transformation of the elements recited therein for generating a shared key. Moreover, step f) has been added to indicate that the results of the simultaneous exponentiation are used to compute the shared key, and each step is amended to indicate that the first correspondent performs same.

Applicants respectfully submit that amended claim 1 constitutes statutory subject matter, and as such complies with 35 U.S.C. §101.

Claim Rejections – 35 U.S.C. §102(b)

Claim 1 was rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,889,865 to Vanstone et al. Applicants respectfully traverse the rejection as follows.

The present application describes, and claims, a method for generating a shared key, that in part, includes a step of computing a simultaneous exponentiation of a first component and a short term public key, and a second exponent and a long term public key. The exponents are computed using private information of the correspondent computing the exponents and public information of a second correspondent, who may also compute the shared key. Claim 1 recites a method for generating such a shared key.

The Vanstone reference cited above describes the well known Menezes-Qu-Vanstone (MQV) protocol for sharing a key between two users of a public key cryptosystem. As described in the background section of the present application, the MQV protocol includes computationally expensive exponentiations required to compute the shared key. The Vanstone reference does not teach, nor even suggest implementing such a protocol using simultaneous exponentiation, which the Applicant have discovered and claimed in the present application.

Accordingly, the Vanstone reference does not teach all elements of claim 1. Therefore, the Vanstone reference clearly cannot anticipate claim 1. Applicants respectfully submit that

claim 1 clearly and patentably distinguishes over the Vanstone reference, and as such is in condition for allowance.

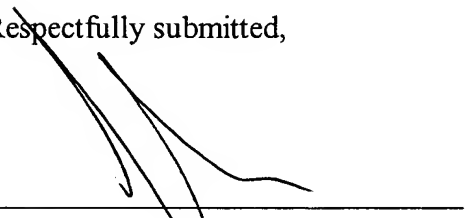
Applicants note that claims 2-8 added in this response are either directly or indirectly dependent on claim 1, and as such are also believed to distinguish over the Vanstone reference.

Summary

In view of the foregoing, Applicants respectfully submit that claims 1-8 submitted in this response constitute statutory subject matter, and clearly distinguish over the Vanstone reference.

Applicants request early reconsideration and allowance of the present application.

Respectfully submitted,



John R.S. Orange
Agent for Applicants
Registration No. 29,725

Date: September 16, 2005

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL